National Cyber Security Awareness Month: Our Shared Responsibility
What Businesses Can Do

You want your business to be a trusted brand. You want to protect your customers and employees. You don't want your valuable intellectual property to fall into the wrong hands. You want to make sure that you contribute to a safe and secure internet to build your business. Consider doing the following during National Cybersecurity Awareness Month:

- Develop internet security policies for your business and train your staff. If you already have internet security policies, review and update them to ensure they address current threats and best practices.

- Review the NCSA/Symantec small business study to see how your Internet security practices stack up against your peers (http://www.staysafeonline.org/content/2009-smb-security-study).

- Hold a brown bag lunch at the office to discuss good cyber security practices, remind employees of company security policies, and answer questions.

- Publish cyber security tips for employees in company newsletters, corporate intranet sites, and/or through posters and handouts in break rooms and other high traffic areas.

- Promote cybersecurity with your customers through your Web site, on customer communications (bills, letters, etc,), or on social media sites such as Twitter and Facebook.

- Set policies that require employees to use long, complex passwords that are changed periodically. If your system allows, require password changes at appropriate intervals.

- Ensure that across your enterprise, operating systems, web browsers, and security suite software are set to update automatically.

- Ensure that all software applications are updated as new versions become available. If you are using a vendor for IT operations be sure they are committed to timely updating as well.

- Create an environment that is supportive of employees raising security concerns.

- Include or update cybersecurity practices in employee handbooks.

- Create a policy regarding the onsite and offsite use of mobile devices and laptops, including whether employees can access work networks from their home computers.   Hold a meeting to discuss this policy to be sure employees understand what's allowable.

- Ask your vendors what steps they take to secure their systems and your data.

- Create a plan in the event of a data loss.

- Do not collect any data that is not critical to running your business, and delete unused and old data.

- Make cybersecurity synonymous with your brand; make sure your customers know what you do to protect their interests.

- Make it policy to turn computers off at night and other down times.

- Show your support for National Cyber Security Awareness Month by putting NCSA's banners for the month on your website.

- Volunteer to teach cybersecurity to young people at your local schools (see NCSA's CSAVE program at www.staysafeonline.org/csave).

- Stay informed on emerging threats and trends in cybersecurity.

- Learn more at www.staysafeonline.org.

- Become a fan of the NCSA's Facebook page (www.facebook.com/staysafeonline).